**Identificador**
**[RFC 2350]**

2025/05/11 **RFC 2350**

**TLP:CLEAR**

## Descripción de Servicios

### 1. Información del Documento

**1.1. Fecha de la última actualización:** versión 2.0, publicada el 15 de mayo de 2025.
**1.2. Listas de Distribución:** No existe un canal de distribución para notificar cambios en este documento. Los cambios son actualizados y publicados en el sitio web.
https://www.colcert.gov.co/800/w3-channel.html
**1.3. Ubicación del Documento:** La versión actual del documento está disponible en el sitio web.
https://www.colcert.gov.co/800/w3-channel.html
**1.4. Autenticación del Documento:** Este documento ha sido firmado digitalmente por la Coordinadora del Grupo ColCERT.

### 2. Información de Contacto

**2.1. Nombre del Equipo:** Equipo de Respuesta a Emergencias Cibernéticas de Colombia ColCERT, CERT Nacional, adscrito al Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
**2.2. Dirección:**
Ministerio de Tecnologías de la Información y las Comunicaciones
Equipo de Respuesta a Emergencias Cibernéticas de Colombia ColCERT
Edificio Murillo Toro Cra. 8a entre calles 12A y 12B
Bogotá D.C., Colombia
**2.3. Zona Horaria:** GMT / UTC -5
**2.4. Número de Teléfono:** +57 601 344 2222
**2.5. Número de Fax:** No existente
**2.6. Otras Comunicaciones:** No existente
**2.7. Direcciones de Correo Electrónico:**
Intercambio de información relativa a incidentes: contacto@colcert.gov.co
Reporte de Malware: malware@colcert.gov.co

Reporte de Phishing: phishing-report@colcert.gov.co

**2.8. Claves Públicas y cifrado de información:** los correos de contacto y claves PGP asociadas se encuentran publicadas en
https://www.colcert.gov.co/800/w3-article-198656.html
**2.9. Miembros del Equipo:** No disponible
**2.10. Más Información:** La información general sobre los servicios proporcionados por el ColCERT y sobre el propio organismo se encuentra publicada en el portal web:
https://www.colcert.gov.co/800/w3-channel.html
**2.11. Horario de Atención:** El equipo de respuesta a incidentes está disponible en los siguientes horarios:
Servicios y consultas: De lunes a viernes de 8:00 – 12:30 y de 14:00 – 17:00.
Incidentes catalogados como muy graves y graves: 7x24
**2.12. Puntos de contacto para la comunidad:** La comunicación entre el Equipo ColCERT y comunidad a los cuales ofrece sus servicios se realiza principalmente a través de:

- Buzón de correo asociado a la temática a consultar
- Teléfonos proporcionados durante el proceso de suscripción o el apoyo a la gestión de incidentes.

## 3. Constitución

### 3.1. Misión

El ColCERT tiene la misión de liderar y coordinar la gestión de incidentes, la identificación de vulnerabilidades, riesgos y amenazas contra la seguridad digital nacional. Actuamos como punto central de contacto y colaboración entre entidades públicas, privadas y la comunidad internacional, fortaleciendo la resiliencia del Estado mediante la compartición de información, el desarrollo de capacidades, la difusión de lineamientos, la identificación de infraestructuras críticas y la promoción de una cultura de seguridad, a través de la cooperación nacional e internacional.
Declaración de +responsabilidad

### 3.2. Comunidad a la que brinda Servicios

Todas las entidades públicas de las ramas del poder ejecutivo, legislativo y judicial, Sector privado y sociedad civil en Colombia.

### 3.3. Patrocinio / Afiliación

El Equipo ColCERT, es un grupo interno de trabajo adscrito al Viceministerio de Transformación Digital del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC

### 3.4. Autoridad

El ColCERT opera bajo el modelo de autoridad compartida en el cual o ejerce una autoridad unilateral o de "comando y control" sobre su comunidad objetivo. En cambio, su autoridad y efectividad se basan en la colaboración, la coordinación, la experiencia técnica y la confianza que genera dentro de esa comunidad.

## 4. Políticas

4.1. Tipo de Incidentes y nivel de soporte: La tipología de incidentes de Seguridad Digital clasificados por el ColCERT, quedan descritos en a taxonomía publicada en el sitio web

https://www.colcert.gov.co/800/articles-198656_taxonomia.pdf

Como CERT Nacional, colabora, apoya y coordina con todas las entidades del sector público y privado en la gestión de incidentes y ofrece servicios adicionales de gestión de vulnerabilidades, análisis situacional y transferencia de Conocimiento.

**4.2. Cooperación, Interacción y divulgación de la Información:** La información gestionada por ColCERT es tratada con absoluta confidencialidad de acuerdo con las políticas y procedimientos del Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC.

Política de Seguridad y Privacidad de la Información
Políticas de Tratamiento de Datos Personales de Ministerio TIC

https://www.mintic.gov.co/portal/inicio/Secciones-auxiliares/Politicas/2627:Politicas-de-Privacidad-y-Condiciones-de-Uso

**4.3. Comunicación y Autenticación:** Los canales de comunicación disponibles para reporte y consultas del ColCERT son:

Línea telefónica Bogotá: +57 601 344 22 22
Intercambio de información relativa a incidentes: contacto@colcert.gov.co
Reporte de Malware: malware@colcert.gov.co
Reporte de Phishing: phishing-report@colcert.gov.co
Los correos de contacto y claves PGP asociadas se encuentran publicadas en
https://www.colcert.gov.co/800/w3-article-198656.html
Red social X: @colCERT

**5. Portafolio de Servicios**

El Portafolio de Servicios del ColCERT es un conjunto integrado y dinámico de capacidades especializadas, diseñado para **fortalecer proactivamente la resiliencia cibernética de la nación.** A través de la **Conciencia Situacional**, proporcionamos inteligencia oportuna sobre el panorama de amenazas. Mediante la **Gestión de Vulnerabilidades**, identificamos y mitigamos debilidades en los sistemas. Con la **Gestión de Incidentes**, ofrecemos una respuesta coordinada y efectiva ante eventos de seguridad. Y a través de la **Transferencia de Conocimiento**, empoderamos a las partes interesadas con las habilidades y la información necesarias para protegerse. En conjunto, nuestro portafolio busca **crear un ecosistema digital colombiano más seguro y confiable.**

**5.1. Línea de servicio: Conciencia Situacional.**

Es un área de servicio fundamental del ColCERT, centrada en la capacidad de anticipar y comprender la evolución del panorama de amenazas y vulnerabilidades que afectan la seguridad digital nacional. Esto requiere la identificación, procesamiento y análisis de información crítica, así como su difusión oportuna a las partes interesadas para facilitar la toma de decisiones preventivas y reactivas. El ColCERT integra información de diversas fuentes y de

sus otras áreas de servicio para proporcionar una visión clara y accionable, fortaleciendo así la capacidad de respuesta y la resiliencia de su comunidad.

### 5.1.1. Colección:

Este servicio del ColCERT se centra en la recopilación exhaustiva de inteligencia estratégica, táctica y operacional, relevante para la seguridad digital nacional. El proceso abarca la identificación, búsqueda, filtrado, organización y almacenamiento de información clave de una variedad de fuentes (Feeds, Tableros de CSIRTAmericas, CERTs, PSIRTs, SOCs, noticias, redes sociales, grupos de mensajería instantánea, informes, herramientas de CTI, etc.), complementando los feeds automatizados. El objetivo principal es mejorar la comprensión del panorama de amenazas, aumentar la visibilidad de la postura de seguridad las entidades publicas y privadas, y en general del país y proporcionar la información necesaria (riesgos, amenazas, vulnerabilidades, IoCs, IoAs, etc.) para el análisis, la comunicación y la fundamentación de decisiones preventivas y reactivas, apoyando así la gestión de incidentes y la mitigación de riesgos.

### 5.1.2. Procesamiento y preparación de datos.

Dada la diversidad de fuentes y formatos de los datos de ciberseguridad, este servicio se centra en su transformación, normalización y validación exhaustiva para asegurar su fiabilidad. La combinación de datos actuales e históricos permite una comprensión contextual más rica. Adicionalmente, se aplican técnicas de procesamiento avanzado (como el análisis de lenguaje natural) para extraer información valiosa de fuentes no convencionales, enriqueciendo el panorama de inteligencia del ColCERT y mejorando su capacidad para anticipar y responder a las amenazas a nivel nacional.

### 5.1.3. Análisis.

El ColCERT utiliza este servicio para transformar datos en inteligencia contextualizada sobre la seguridad digital nacional. A través de la evaluación de la situación actual en relación con patrones esperados, se identifican posibles riesgos para los activos críticos. El análisis profundo de datos actuales e históricos revela la naturaleza y el origen de eventos, así como sus implicaciones presentes y futuras. La incorporación de diversas fuentes de información enriquece la comprensión y permite al ColCERT generar conocimiento accionable para la prevención y respuesta a amenazas.

### 5.1.4. Comunicación.

A través de su servicio de comunicación, el ColCERT genera y difunde inteligencia procesada y analizada para mejorar la comprensión del panorama de la seguridad digital en Colombia. Un componente fundamental es la generación de alertas y advertencias, mediante las cuales se comunica información crítica sobre amenazas, ataques, nuevas vulnerabilidades y riesgos de seguridad digital, incluyendo alertas provenientes del monitoreo de inteligencia de amenazas.

El propósito es aumentar la preparación y capacidad de respuesta de las partes interesadas, proporcionando recomendaciones de mitigación para fortalecer su seguridad y reducir su exposición.

### 5.2. Gestión de Vulnerabilidades

El ColCERT, a través de su Área de Servicio de Gestión de Vulnerabilidades, se encarga del descubrimiento, análisis y gestión proactiva de vulnerabilidades de seguridad, tanto nuevas como existentes, en los sistemas de información. Un componente crucial es la detección y respuesta coordinada a vulnerabilidades conocidas para prevenir su explotación. Es importante distinguir que, si bien la "Respuesta a Vulnerabilidades" es una actividad fundamental (como el escaneo y el parcheo), esta se enmarca dentro de un servicio más amplio de Gestión de Vulnerabilidades que puede involucrar diferentes equipos y procesos dentro del ColCERT.

#### 5.2.1. Descubrimiento de Vulnerabilidades de Fuentes Públicas.

Una función proactiva del ColCERT para identificar tempranamente conocidas y nuevas vulnerabilidades de seguridad mediante la recopilación de información a través de diversas fuentes públicas y de terceros. La información recopilada por personal especializado se organiza y analiza, integrándose con los datos de herramientas de huella digital y protección demarca, para alimentar los servicios de Gestión de Vulnerabilidades y Alertas Tempranas del ColCERT.

#### 5.2.2. Recepción de Informes de Vulnerabilidad.

El ColCERT facilita la notificación de vulnerabilidades de seguridad a través de canales definidos para recibir informes de una amplia gama de fuentes, incluyendo sus constituyentes, la comunidad de investigación en seguridad, proveedores de tecnología, PSIRTs y otros CSIRTs. La información recibida puede abarcar desde los dispositivos afectados y los requisitos de explotación hasta el impacto potencial y las soluciones propuestas. Este servicio asegura que la valiosa información sobre vulnerabilidades se capture y se utilice eficazmente en los procesos de gestión y respuesta del ColCERT, complementando la información obtenida a través de la recepción de informes de incidentes.

#### 5.2.3. Análisis de Vulnerabilidades (Bajo Demanda).

A través de este servicio, el ColCERT realiza análisis de vulnerabilidades a petición de las organizaciones para descubrir debilidades en diversos entornos tecnológicos: infraestructura on-premise, nube, Directorio Activo, y servicios web. Empleando herramientas licenciadas y open source, el nivel de análisis se adapta a la capacidad de seguridad del solicitante, ofreciendo un informe básico para entidades con CISO/Encargado y un análisis más profundo para aquellas sin esta figura.

### 5.2.4. Reporte de Vulnerabilidades:

Servicio del ColCERT que entrega reportes derivados de la recepción de informes y análisis de vulnerabilidades solicitados por entidades públicas y privadas. El objetivo principal es proporcionar información sobre la identificación de vulnerabilidades críticas, altas, medias e informativas, para facilitar el establecimiento de planes de mitigación, mejorar su postura de seguridad, cerrar la brecha en la superficie de ataque y evitar incidentes que puedan impactar sus operaciones y la continuidad de los servicios a la ciudadanía, a través de los canales de comunicación establecidos y garantizando la confidencialidad de la información.

## 5.3. Gestión de Incidentes de seguridad Digital

El ColCERT, con su posición y experiencia únicas, ofrece un servicio fundamental de Gestión de Incidentes de Seguridad Digital. Esto implica la recopilación, evaluación y análisis técnico profundo de incidentes y artefactos. A partir de este análisis, se generan recomendaciones de mitigación y recuperación, brindando apoyo en su aplicación y coordinando con entidades externas para una respuesta efectiva y la prevención de futuros incidentes. La experiencia especializada del ColCERT también es crucial para apoyar la gestión de crisis de seguridad digital en el país.

### 5.3.1. Recepción de reportes de Incidentes de Seguridad Digital.

Servicio del ColCERT dedicado a recibir reportes de incidentes de seguridad digital clasificados como Muy Graves o Graves, según el procedimiento de gestión de incidentes del ColCERT y el lineamiento de gestión de incidentes del MSPI, provenientes de entidades públicas y privadas. Estos reportes se reciben a través de los canales de comunicación establecidos por el ColCERT.

### 5.3.2. Triaje y Procesamiento de Incidentes de Seguridad Digital.

Este servicio se enfoca en la revisión y clasificación inicial de los reportes de incidentes de seguridad digital para comprender su naturaleza e impacto en los activos de información a nivel nacional, considerando también la clasificación proporcionada por la organización afectada. Tras esta evaluación preliminar, se prioriza el incidente y se define la acción de seguimiento, que puede ser la convocatoria a una reunión de contexto para recabar más detalles.

### 5.3.3. Mitigación y Recuperación

El ColCERT ofrece este servicio para contener eficazmente los incidentes de seguridad digital, minimizando y reduciendo las pérdidas operacionales y económicas. El objetivo es lograr una recuperación oportuna de los servicios impactados, prevenir la recurrencia de ataques mediante la eliminación de las causas raíz y fortalecer la postura general de ciberseguridad en las entidades públicas y privadas. El servicio comprende la ejecución y el seguimiento de las acciones necesarias hasta la resolución del incidente o la identificación de nueva información que requiera una revisión de la estrategia de respuesta.

### 5.3.4. Establecimiento del Plan de Respuesta.

Servicio del ColCERT para definir y aplicar un plan coordinado con la entidad afectada, con el fin de restaurar la integridad de los sistemas comprometidos y devolver los datos, sistemas y redes a un estado operativo normal. El plan busca restablecer la funcionalidad completa de los servicios impactados, evitando la recreación de las condiciones que permitieron la explotación inicial. Se considera el impacto empresarial y los requisitos de mitigación y recuperación, y el plan se revisa continuamente a medida que se obtiene nueva información, asegurando una respuesta eficaz y coordinada a nivel nacional.

El ColCERT ofrece una protección integral a nivel nacional a través de dos capacidades clave: la **Protección de Dominios e Investigación de DNS**, que actúa como una capa preventiva al analizar el tráfico DNS para detectar y predecir amenazas, además de mitigar ataques en curso mediante la restricción de conexiones maliciosas. Complementariamente, la capacidad de **Detección y Respuesta contra Malware EDR** proporciona una monitorización continua y una respuesta activa a las amenazas que alcanzan los endpoints y las redes de entidades públicas y privadas, apoyando la recuperación tras incidentes y fortaleciendo su seguridad.

### 5.3.5. Coordinación de Incidentes de Seguridad Digital.

El ColCERT ofrece este servicio para gestionar la respuesta a incidentes de seguridad digital a nivel nacional, asegurando una comunicación eficaz y oportuna entre todas las partes interesadas (Instancias Ciber). Esto implica recibir y distribuir información relevante, hacer seguimiento al progreso de las acciones de mitigación y recuperación, garantizar la implementación del plan de respuesta y abordar las modificaciones necesarias debido a nueva información o retrasos. Así mismo y según el modelo de gobernanza de seguridad digital (Decreto 338 del 2022), informar los incidentes de seguridad digital que tengan un impacto nacional o que afecten la infraestructura critica cibernética.

### 5.3.6. Apoyo a la Gestión de Crisis

El ColCERT actúa como un recurso crítico para entidades públicas y privadas en situaciones de crisis de seguridad digital, ofreciendo su valiosa experiencia, sus servicios establecidos y su red de contactos con otros expertos y CSIRTs, en su rol como CERT Nacional de Colombia. Este apoyo busca facilitar la mitigación de la crisis y asegurar la disponibilidad del ecosistema digital del país y su red de aliados para la recuperación de las operaciones.

### 5.3.7. Análisis de Artefactos

El ColCERT ofrece dos servicios relacionados con el análisis de software malicioso:

1. **Análisis en Sandbox:** Para la gestión de incidentes de seguridad digital, el ColCERT analiza archivos en una sandbox, generando informes técnicos detallados sobre el comportamiento de software potencialmente malicioso e identificando Indicadores de Compromiso (IoC).
2. **Análisis Web (DetectIC):** Para facilitar la detección de amenazas por parte del público en general y los equipos técnicos de entidades públicas, el ColCERT ofrece la

herramienta web de análisis en línea DetectIC. Este servicio examina archivos y URL en busca de cargas maliciosas, notificando de manera general su peligrosidad.

## 6. Transferencia de conocimiento

Es un área de servicio esencial del ColCERT, aprovechando su posición privilegiada para recopilar datos relevantes, realizar análisis detallados e identificar amenazas, tendencias y riesgos. El ColCERT genera y difunde las mejores prácticas operativas actuales para concientizar y capacitar a las organizaciones en la detección, prevención y respuesta efectiva a incidentes de seguridad, contribuyendo así a elevar el nivel general de ciberseguridad en Colombia.

### 6.1. Concientización en Seguridad Digital comunidad en General

Proporcionar a la ciudadanía las herramientas y la educación esencial para fortalecer la seguridad de sus entornos personal, familiar y profesional, así como la de sus entidades y organizaciones, a través de una estrategia de concienciación fundamentada en la gestión de riesgos.

### 6.2. Capacitación Gestión de Incidentes Basico, Intermedio y Avanzado

Programa de entrenamiento diseñado para equipar a los equipos de respuesta a incidentes de seguridad digital y directores de TI de entidades públicas y privadas con las habilidades necesarias para llevar a cabo acciones preventivas y reactivas. Esto incluye el análisis, identificación, clasificación, contención, erradicación, recuperación y gestión post-incidente.

### 6.3. Concientización Seguridad Digital Directivos

Programa estratégico para sensibilizar a la alta dirección de entidades públicas y privadas sobre la naturaleza transversal de la seguridad digital en todos los procesos organizacionales. Se enfatiza la importancia de establecer una estrategia y una postura de seguridad robustas para mitigar la materialización de riesgos y prevenir incidentes que puedan generar impactos legales, financieros y reputacionales significativos.

## 7. Formas de notificación de incidentes

La notificación de incidentes puede realizarse mediante:

Línea telefónica Bogotá: +57 601 344 22 22
Intercambio de información relativa a incidentes: contacto@colcert.gov.co
Reporte de Malware: malware@colcert.gov.co
Reporte de Phishing: phishing-report@colcert.gov.co
Los correos de contacto y claves PGP asociadas se encuentran publicadas en
https://www.colcert.gov.co/800/w3-article-198656.html

**8. Disclaimer**

El Equipo COLCERT no se responsabiliza del mal uso que pueda darse de la información aquí contenida.

## Canales de Atención

Si tiene desea reportar un incidente de seguridad digital, puede comunicarse con el COLCERT, a través de los siguientes canales:

Bogotá: +57 601 344 22 22

contacto@colcert.gov.co.

@colCERT